総務省 学術雑誌『情報通信政策研究』 第2巻第2号
Journal of Information and Communications Policy Vol.2 No.2

論文（査読付）

オンライン広告におけるトラッキングの現状とその法的考察 ―ビッグデータ時代のプライバシー問題にどう対応すべきか

若江雅子[1]、森亮二[2]、吉井英樹[3]

要　旨

インターネット広告の重要性が増している。その広告費（媒体費＋制作費）は2007年の6,003億円から2017年には1兆5,094億円に増え、新聞広告の5,147億円の3倍、テレビメディアの1兆9,478億円にも迫る勢いである[4]。その強みは、ウェブの利用履歴から利用者一人ひとりの趣味嗜好・性別・年齢・居住地などに関する情報を取得し、それに沿った広告を表示できることにあるだろう。興味関心連動型などと呼ばれるこうした広告は、かつてはAmazonや楽天のようなECサイトが、自社ネットワークにアクセスした顧客から利用履歴を直接取得して、その顧客の閲覧画面に広告を表示する形で行われていたが、近年は、利用履歴を顧客から直接取得しなくても同様の広告を掲載することが可能になっている。それは、クッキーや広告IDなどブラウザや端末の識別子に紐付いた利用履歴が、各種プラットフォームを通じて流通しているためである。

個人情報保護法は、個人情報を第三者に提供する場合、原則として本人の同意を義務づけている。しかし、クッキーや広告IDなどのブラウザや端末の識別子に紐付いた情報は、それ単体では個人識別性がないとして、個人情報としての規制を受けない。このため、利用者の同意を得ないまま、第三者に提供することが可能であり、実際に、広告事業者の間で広範にやり取りされているのが現状である。だが、これらの情報は、提供先が保有する情報と突合された場合に個人情報に変わり得る性質のものである。では、提供元では個人識別性を有さない情報が、第三者に提供され、その結果、提供先で個人識別性を有する情報となった場合、第三者提供の規制を受けるのだろうか。こうした問題については、必ずしも明確な整理がなされていないのが実情である。

本論文は、ウェブサイト利用者の使用するブラウザや端末の識別子に紐付いた情報が、利用者が提供を想定していない事業者に取得され、事業者が保有する他の情報と突合された結果、個人情報となる現状について検証し、こうした情報の流通について現行の個人情報保護法により規制が可能かどうか検討を試みるものである。

キーワード：クッキー、フェイスブック、DMP、個人情報保護法、第三者提供

１．はじめに

2018年春、データ分析会社であるケンブリッジ・アナリティカが8,700万人ものフェイ

[1] 情報セキュリティ大学院大学修士課程。
[2] 英知法律事務所。
[3] ソフトバンク株式会社。
[4] 電通「2017年日本の広告費」（2018年2月22日）。
http://www.dentsu.co.jp/news/release/2018/0222-009476.html

スブック（以下、「FB」と略。）ユーザーのデータを 2016 年アメリカ大統領選キャンペーンなどに利用していたという疑惑が浮上した。世界的に大きな波紋を広げたこの問題は、オンラインを通じて収集される個人情報がいかに膨大であり、使いようによっては個人の政治思想や心理状態に働きかけて世論を操作しうるものであると示したといえよう。

しかし、そもそもこれらの大量の個人情報が一体どのように収集されたのか、私たちは把握しているだろうか。一部は FB 利用者が FB 上で自ら入力したプロフィールや投稿などに基づくものであるが、それ以外にも、FB が他の事業者から購入したデータや、私たちが FB 以外のウェブサイトを閲覧したり何らかの物品やサービスを購入したりした際のウェブ上の行動履歴を集めたものも大量に含まれている。多くの利用者は、自分たちが直接提供したわけでもない自分の個人情報を FB がこれほど大量に保有していたことに驚いたのではないか。だが、これは FB だけの問題ではないのである。

近年、インターネット広告は急速にその存在感を増し、我が国でもその広告費（媒体費＋制作費）は 2007 年の 6,003 億円から 2017 年には 1 兆 5,094 億円に増えた。新聞広告 5,147 億円の 3 倍、テレビメディアの 1 兆 9,478 億円にも迫る勢いである [5]。その強みは、ウェブの利用履歴から利用者一人ひとりの趣味嗜好・性別・年齢・居住地などに関する情報を取得し、それに沿った広告を表示できることにある。興味関心連動型などと呼ばれるこのような広告配信が可能となったのは、広告事業者などが私たちのウェブ上の行動履歴を、広告 ID やクッキーなどという使用端末やブラウザの識別子と紐付けて広く収集し、事業者間で流通させているからである。

しかし、多くのウェブサイト利用者はそのことに気づいておらず、とりわけ日本では、こうした情報取得の窓口となっているウェブサイト運営者さえ、その実情を把握していないことも少なくない。その一因は、収集の「入り口」で取得される情報が、クッキーや広告 ID などブラウザや端末の識別子に紐付けられた情報であり、我が国の個人情報の保護に関する法律（以下、「個人情報保護法」。）では個人情報と位置づけられていないという事情にあろう。しかし、個人識別性は原則として相対的なものである。収集の時点においては個人識別性を有しない情報（非個人情報）であっても、その情報に他の情報が突合されることによって、個人識別性を有する情報（個人情報）に変わり得るものであり、その結果、個人の権利利益を侵害する可能性は十分に存在するのである。

本研究では、まず、こうした国内の実態を FB の「いいね！ボタン」などのソーシャルプラグインを巡る実態や、DMP（Data Management Platform）事業者によるデータ提供の現状などについて調査し、端末やブラウザに紐付いた個人に関する情報が、どのように個人情報に変わりうるのか、そしてそれはどのように本人の権利利益を侵害しうるのかを検証する。その上で、これらの現状に対して個人情報保護法を中心とする現行法がどう対応しうるのか、①取得の主体としての規制と、②第三者提供の規制について考察する。

２．個人情報の定義と端末等を識別する情報に対する規制の検討状況

個人情報保護法における個人情報とは、生存する個人に関する情報で、特定の個人が識

[5] 前注 4。

別できるものである [6]。ただし、その情報自体で特定の個人を識別することができなくても、他の情報と容易に照合することで特定の個人を識別できれば個人情報である [7]。例えば、「いろは商事営業部、甲山乙男」という情報は個人情報である。一方、「いろは商事　社員番号 12345」という情報は、社員番号の名簿を保有するいろは商事にとっては個人情報であるが、名簿を保有しない企業にとっては個人情報ではない。このように、個人識別性は相対的に判断されるものであり、同じ情報でも、A にとっては個人情報でないが、B にとっては個人情報であるということがあり得るのである。

情報化社会の到来により、大量で多様な個人に関する情報がインターネット上にあふれ、容易に検索可能になった今、特定の個人が識別されない情報であっても、他の情報と結びつくことによって個人が特定される恐れはかつてに比べ格段に高まっている。ことに、1 人が 1 台以上の情報端末を日常的、継続的に使用する状況では、使用端末などに紐付く個人に関する情報については、その懸念は特に増しているといえよう。

そのような問題意識から、改正個人情報保護法（2017 年 5 月施行）の検討段階で高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）の有識者会議「パーソナルデータに関する検討会」では、個人情報保護法の規制対象に新たに「（仮称）準個人情報」の概念を導入することが提案された [8]。これは「個人または個人の情報通信端末（携帯電話端末、PC 端末等）等に付番され、継続して共用されるもの」などを、個人情報に準じる形で保護する旨の提案であり、同検討会の下に設けられた「技術検討ワーキンググループ」に技術的な検討が託された。同ワーキンググループは 2014 年 5 月、中間報告 [9]をまとめ、「本人又は本人の所有物と密接性があるもの」「一意性/単射性があるもの」「共用性があるもの」「変更可能性/不変性/利用停止可能性については容易に変更できないもの」の指標を掲げ、こうした性質をもつ識別子を準個人情報として扱うべきと指摘した。具体的には、免許証番号、パスポート番号、健康保険証番号、クレジットカード番号、メールアドレス、車両番号、固定電話番号、携帯電話番号、情報通信端末シリアルナンバー（携帯電話シリアルナンバー等）、MAC アドレス、情報通信端末 ID、IC カードの固有 ID、ソフトウェアシリアル番号などである [10]。

しかしながら、改正法には「準個人情報」の概念は採用されなかった。改正法では、個人情報の概念に新たに「個人識別符号」（同法第 2 条第 2 項）が、それ単体で個人情報となるものとして盛り込まれたが、この中には、情報端末を識別する ID は含まれていない。

---

6 個人情報保護法第 2 条。

7 園部逸夫・藤原静雄編『個人情報保護法の解説』（ぎょうせい、2018 年）62 頁。容易に照合ができるとは「特別の費用や手間をかけることなく、すなわち事業者において通常の業務における一般的な方法で、特定の個人を識別する他の情報との照合が可能な状態である」としている。

8 第 7 回パーソナルデータに関する検討会　配付資料 1-2（詳細編）（2014 年 4 月 16 日）。https://www.kantei.go.jp/jp/singi/it2/pd/dai7/siryou1-2.pdf

9 技術検討ワーキンググループ「『（仮称）準個人情報』及び『（仮称）個人特定性低減データ』に関する技術的観点からの考察について（中間報告）」（2014 年）。https://www.kantei.go.jp/jp/singi/it2/pd/dai9/siryou2-2.pdf

10 クッキーについては、ブラウザの利用者が自ら消去することが可能であることなどから、引き続き検討を要すると位置づけられた。

改正法成立 4 か月前の国会でも、政府は「単に機器に付番されるような、例えば携帯電話の通信端末 ID は個人識別符号には該当しない」と答弁している [11] 。結局、情報端末の ID などに紐付いた個人の履歴情報は、他の情報と照合することで個人識別性が生じる場合を除き、保護対象とされないこととなっているのである [12]。

しかし、EU では個人データ（Personal Data）を識別された又は識別されうる自然人に関するあらゆる情報と定義し、情報端末やブラウザを識別する ID やクッキー、IP アドレスなども含めてきた。これは 2018 年 5 月に適用開始された GDPR（General Data Protection Regulation：一般データ保護規則）でも同様の定義（第 4 条第 1 号）[13]とされている。こうした状況も踏まえ、日本国内でも、情報端末を識別する ID を保護対象とすべきだったとの批判は依然としてある [14]。

３．広告事業者によるウェブ行動履歴の収集

３．１．アドテクノロジーの変遷

世界で最初のオンライン広告は 1994 年、Wired 誌のデジタル版「Hot Wired」に掲載された AT&T 社のバナー広告で [15]、日本では 2 年後の 1996 年、「Yahoo！JAPAN」への掲載が最初だとされる [16]。当時は、媒体（メディア）の固定された広告枠にあらかじめ決められた広告を掲示する「純広告」が中心だったが、次第に広告枠を外部化し、「アドサーバー」で広告配信や管理を行う方式に移行していく。これは、媒体のウェブコンテンツを送り出すウェブサーバーとは別に、外部に置かれたアドサーバーから広告だけを配信する仕組みである。広告配信がウェブサイトのアクセスから切り離されることで、柔軟な運用が可能となり、配信可能数（在庫）や配信期間の管理、どの広告が何回表示されて何回クリックされたかという効果測定などの技術も進んでいった [17]。アドサーバーは当初、媒体社が管理していたが、これを広告会社など第三者が保有・管理する「第三者配信」の仕組み

---

11 第 189 回国会・内閣委員会第 4 号（2015 年 5 月 8 日）向井治紀・内閣官房内閣審議官の答弁。
http://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000218920150508004.htm

12 例えば、スマートフォンなどの通信機器に割り振られた固有の識別子 MAC アドレスは、通信キャリアが保有する契約者情報と照合できる場合などには個人情報となるが、小売店で客の動きを把握するために、客のスマートフォンの MAC アドレスを受信し、位置情報を追跡するケースなどでは、小売店は個人情報として扱っていない。

13 個人情報保護委員会「一般データ保護規則の条文」（同委員会の和訳）。
https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

14 高木浩光「個人情報保護から個人データ保護へ～民間部門と公的部門の規定統合に向けた検討(1)」情報法制研究第 1 号（2017 年 5 月）88 頁。「達成できなかった課題とは、一つは、いわゆる「端末 ID」を識別子として蓄積される個人に関する履歴情報を保護対象とすることが検討されながらも実現しなかったこと」。

15 日経 BP「日経クロステックアクティブ・知っておきたい BtoB マーケティングのきほん」（2016 年 3 月 24 日）。
https://tech.nikkeibp.co.jp/it/atclact/active/15/051900050/022400024/

16 広瀬信輔『アドテクノロジーの教科書』（翔泳社、2016 年）2 頁参照。

17 日本インタラクティブ広告協会「インターネット広告の基本実務 2016 年度版」。

が主流となっていくと、運営母体の異なる様々なサイトの広告をアドサーバーでネットワーク化する「アドネットワーク」が形成されていくようになる。アドサーバーを管理する広告会社がサイト横断的に広告の受注を請け負うことができるため､広告主側にとっては、アドネットワーク事業社１社への発注で複数サイトに同時配信できるなど効率的な出稿が可能になり、媒体社にとっても、販路のない広告主からの受注や、配信管理の負担軽減化などの効果が期待できるようになった。また、ユーザーの行動を複数の媒体にわたって追跡し、データを取得することが可能になり、ターゲティング広告のメニューも多彩になっていった。ただ、これは閲覧者からすれば、自らの意志でアクセスしたウェブサイトとは別に、意図しないまま第三者の管理するアドサーバーにもアクセスし、気づかないうちにウェブ上の行動履歴を取得されることとなるのである。

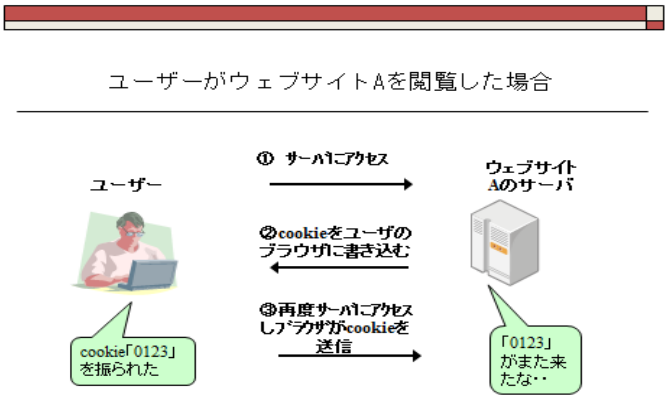
効率的で効果的な広告配信を目指すこうした動きのなかで、大きな存在感をもつようになったのが､「オーディエンスデータ」と呼ばれる、ユーザーの閲覧履歴や購買履歴、デモグラフィック情報（性別、年齢、居住地域、所得、職業、家族構成など）などである。媒体や広告面だけでなく、閲覧者ごとに興味関心や必要性、購買力などに合った広告を配信する手法が注目され、それにつれてユーザーのデータを事業者間で交換するデータエクスチェンジという仕組みも登場した。「DMP（Data Management Platform)」とよばれる、ユーザーデータの収集・蓄積・統合・分析を行うプラットフォームも現れ、企業が自社で蓄積したデータを活用するために用いるプライベート DMP のほか、第三者から集めたデータを統合して第三者に提供するパブリック DMP も存在する。

３．２．JavaScript とクッキーによるユーザーデータの統合と蓄積

では、こうしたユーザーデータは、具体的にどのように集められ、事業者間をどう流通するのか。現在主流となっている手法の一つは、簡易プログラム JavaScript と、ブラウザを識別するクッキーを活用したものである。

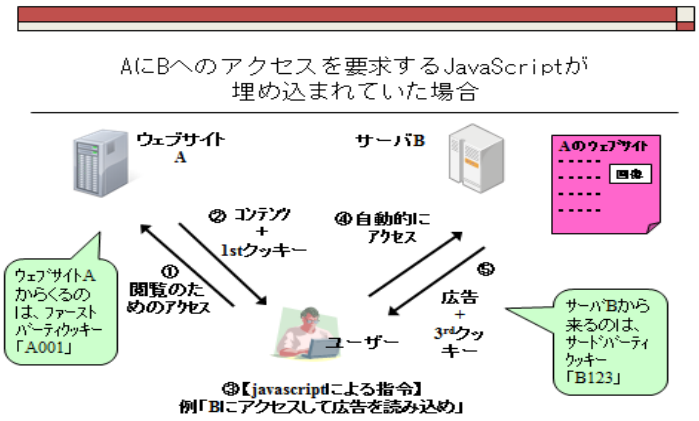
クッキーとは、ウェブサイトの提供者が、閲覧者のコンピューターにブラウザを介して一時的に書き込むデータで、閲覧者の識別や認証のために使われるものである。例えば、ユーザーがウェブサイト A を閲覧した際、A のサーバーはユーザーのブラウザに対してクッキーを送りつける。二度目以降に A を閲覧すると、ブラウザはこのクッキーを送り返すため、A のサーバーは同じ閲覧者が訪問したことを確認できる（図 1)。このクッキーはユーザーの訪問したウェブサイトが発行したクッキーで「ファーストパーティクッキー」と呼ばれる。クッキーの発行元ドメインは、訪問サイトのドメインと一致する形である。

図 1. クッキーの仕組み（ファーストパーティクッキー）作成・森亮二



これに対し、ユーザーが訪問したウェブサイトやサービスの運営主体以外の事業者が発行するクッキーを「サードパーティクッキー」と呼ぶ。例えば、ウェブサイト A と広告事業者 B とが提携し、A のウェブサーバーのウェブ文書（HTML）上に B が JavaScript を設置してもらい、A を閲覧したブラウザに対し、「B のサーバーにアクセスしろ」などの指示をすると、このユーザーのブラウザは B のサーバーにアクセスする。すると B のサーバーもこのユーザーにクッキーを発行する。これがサードパーティクッキーで、ユーザーはアクセスしたつもりのない B から、ブラウザを識別される状態になる（図 2）。

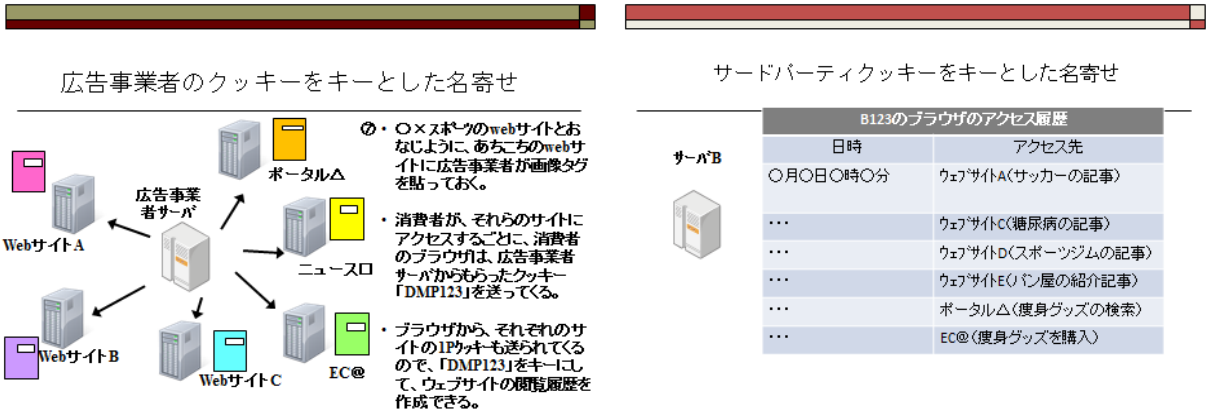
図 2. クッキーの仕組み（サードパーティクッキー）作成・森亮二



この時、B はファーストパーティクッキーと統合したり、リファラ（ブラウザがサーバーに送信する、リンク元サイトの URL）を参照したりすることによって、このユーザーがサイト A からの訪問者であることが分かる。もし、B が、サイト A ばかりでなく、サイト C やサイト D やサイト E などにも同じように JavaScript を埋め込んで、閲覧ユーザーにアクセスを要求すると、B はユーザーが A や C や D や E を閲覧したことも把握できる。B が多くのサイトと提携すればするほど、ユーザーのウェブ上の様々な行動履歴がクッキーを介して統合されていくことになる。JavaScript の指示内容によっては、単にアクセス要求だけでなく、ポインタの位置やクリックの有無、入力内容などの情報を送信させるこ

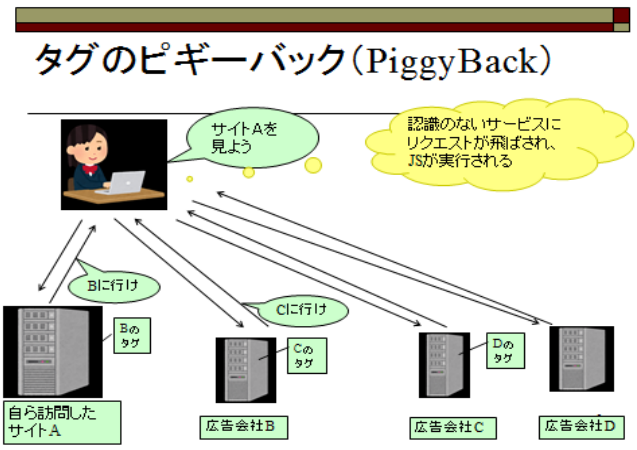
とも可能で、例えば、ニュースサイトでどんな記事をどのくらいの時間をかけて読んでいたのか、何をクリックしたのか、どんな言葉を検索していたのか、どんな商品を購入したのかといった情報を得ることも可能である。しかし、ユーザーにすれば、ブラウザに紐付く情報とはいえ、自らアクセスしたわけでもない B に、興味関心に関する情報を把握されてしまうことになる（図 3)。

図 3. サードパーティクッキーをキーとした名寄せ　作成・森亮二



さらに状況を複雑にしているのが、サーバー側でブラウザに対し指示ができるという JavaScript の特性を使った JavaScript の「入れ子構造」である。サイト運営者が、広告会社などと提携して閲覧者をその広告会社のサーバーにアクセスさせる JavaScript を設置する際、その広告会社のサーバーに、新たに別の広告会社などへのアクセスを指示する JavaScript を設置するといった手法で、広告業界では「ピギーバック」などと呼んで広く活用されている　(図 4)。

図 4.JavaScript タグのピギーバック　作成・若江雅子



この結果、サイト運営者としては設置を許可した覚えのない第三者のサーバーにも、閲覧者のブラウザに JavaScript を実行することを許し、各種情報を送信させることになる。

例えば、タレントのコマーシャル起用で知られる大手スポーツジム運営会社の場合、2018 年 5 月の調査時点でサイト閲覧すると閲覧者のブラウザは 86 の広告会社や解析会社などにアクセスし、情報を送信することとなっていたが 、執筆者がこのジム運営会社にたずねたところ、把握していたのは代理店 1 社に依頼した 6 事業者の 11 の JavaScript のみであり、残る 75 の情報送信先については気づいていなかった。

このような多数のサードパーティクッキーに紐付けられたユーザーの情報は、現在、広告事業者の間で広く共有されるようになっている。「クッキーシンク」と呼ばれる手法で、それぞれ管理しているクッキーを同期させ、ID を連携させることで、それぞれの保有するユーザーのデータを拡大しているのである。

４．クッキーデータが個人情報に変わるケース

４．１．FB の「いいね！」ボタン問題

これまで述べてきたようなユーザーのウェブ行動履歴の収集は、収集時点において、ブラウザを識別するクッキーに紐付いた情報である。２．で述べたように、ブラウザを識別する情報は単体では個人情報保護法上の個人情報ではなく、ゆえに、こうした収集をウェブ利用者の同意なく行われることが法的に許容されてきたといえよう。

しかし、前述の通り、個人識別性は相対性をもつ。ある時点では非個人情報であっても、個人情報を保有する事業者の下で他の情報と突合されるなどすれば、個人情報に変わり得る。その典型が、FB の「いいね！ボタン」などのソーシャルプラグインを巡る問題である。

「いいね！ボタン」は、FB 上で会員が写真やコメントなどに肯定的な意志を示すために使われるだけでなく、FB 以外のウェブサイトにも設置できるソーシャルプラグインである。サイトの訪問者が、そのコンテンツに関心や興味を抱いたときにクリックすれば、クリックされた回数が表示されるため、サイト運営者は、コンテンツに対する訪問者の関心度が分かる。一方、クリックした訪問者は、そのコンテンツを FB の友達と共有したり、コンテンツの更新情報を受けたりすることができる。その利便性の高さから、広く普及しており、データ解析会社「データサイン」の調査では 2018 年 1 月現在、国内約 18 万サイト中、3 万 1,252 サイトで設置が確認された[18]。また、2018 年 1 月末現在、国内売上高トップ 100 の上場企業の半数以上で設置され[19]、中央省庁など公的機関のウェブサイトでは、首相官邸、外務省、財務省、警察庁、国家公安委員会、農水省、陸・海・空自衛隊、会計検査院で設置が確認[20]された。

しかし、「いいね！ボタン」は、その名称や形状から、ボタンをクリックした場合にのみ何らかの情報が FB に送信されると閲覧者に想像させるが、実際には、クリックの有無に関係なく、ボタンが設置されたウェブサイトを閲覧しただけで FB のサーバーにアクセスし、ブラウザの閲覧情報などを送信するものである。「いいね！ボタン」は、外部のウェブ

---

18 株式会社 DataSign「Web サービス調査レポート 2018.1」（2018 年 2 月 1 日）。
https://datasign.jp/blog/datasign-report-docodoco-20180201/

19 読売新聞「「いいね！」ボタン設置サイト　閲覧だけで「個人情報」送信　保護法抵触か」（2018 年 2 月 25 日）。

20 前掲注 19。

サイト運営者が、FB の公開する「いいね！ボタン」用の JavaScript をウェブ文書に貼り付けることによって実装される。つまり、その実態は、前述した第三者によるサードパーティクッキーの収集と同様、JavaScript を使ってサイト閲覧者のブラウザに紐付いた情報を FB に集めるためのものなのである。

ここで問題となるのが、実名登録による利用を原則としている FB の場合、FB は会員の個人情報を保有している点である。このため、サイト訪問者が FB の ID を持っており FB にログインした状態にある場合、FB 側は、そのブラウザに発行したクッキーからどの会員のブラウザなのかを照合することが可能となる。仮にこの時点でログインしていなくても、次回に FB を利用する際、この訪問者がクッキーを消去しない限り、過去の訪問履歴と照合することが可能となる。このような仕組みから、閲覧ブラウザが FB に送信する情報は非個人情報のクッキーデータであるが、FB が取得する時点で FB 利用者分については個人情報になると解される。

FB によれば、国内の有効ユーザー数は 2017 年 9 月時点で 2,800 万人[21]であるという。また、総務省が 13 歳から 69 歳までの男女 1,500 人を対象にした調査では 32.3%が FB を利用していると回答[22]している。前述の通り、国内の少なからぬウェブサイトが「いいね！ボタン」を設置していることを考えると、膨大な閲覧履歴が個人情報と紐付いて FB に集積されていることになる。

これに関して問題と思われるのは、以下のような点である。

第一に、利用者への周知の問題である。「いいね！ボタン」をクリックした場合に、その情報が FB に送信されることまでは想像の範囲内といえるかもしれないが、FB と資本関係がないなど一見無関係と思われる企業等のサイトを閲覧しただけで FB に閲覧情報が送られるということは、一般の利用者には予想がつかないであろう。

2018 年 3 月時点で、FB の国内広報担当に対し、FB のソーシャルプラグインが設置されたサイトを会員が閲覧した場合に送信される情報についてたずねたところ、「個人情報として扱っており、プライバシーポリシーでも説明している」と回答した。その時点で FB は「サービス(いいね！ボタン、Facebook ログイン、広告、効果測定など)を利用した外部ウェブサイトや外部アプリを利用者が閲覧または使用したとき、弊社はその情報を収集します。 これには利用者がアクセスしたウェブサイトやアプリ、それらのウェブサイトやアプリ内でのサービスの利用状況に関する情報、またアプリやウェブサイトの開発者や発行元が利用者や弊社に提供する情報が含まれます」と記載していた[23]。

しかし、これについてはいくつかの問題があった。第一に、具体的にどのような情報が収集されるのかはっきりせず、また、「いいね！ボタン」がどのウェブサイトに設置されているのかも書かれていなかった点である。

第二に、利用者が収集を拒否することがほぼ不可能な点である。前述のように、利用者

---

[21] FacebookJapan2017 年 9 月 14 日発表。

[22] 総務省「情報通信メディアの利用時間と情報行動に関する調査」(2017 年 7 月)。

[23] この記載は、FB のトップページに表示される「プライバシー」のハイパーリンクをクリックすると「データに関するポリシー」のページが表示され、その中の「Facebook が収集する情報の種類」の中の 6 番目のカテゴリ「Facebook サービスを使用するウェブサイトやアプリからの情報」にあった。

にはどのサイトに「いいね！ボタン」が設置されているかは事前には分からず、閲覧によってボタン設置に気づいた時には、もう FB に閲覧情報は提供された後である。また、オプトアウトなど事後的に拒否する仕組みも用意されていなかった。

第三に、FB は「いいね！ボタン」などの設置基準を定めておらず、収集情報の機微性についての配慮に欠ける点である。設置サイトの中には、アダルトサイトなど閲覧の事実を他人に知られたくないと考えるようなサイトや、自分や家族が特定の病気にかかっていることを推測させるような医療情報サイトなども含まれていた[24]。

４．２．FB 問題の法的評価

FB のこのような情報収集の法的評価については、プライバシー侵害と個人情報保護法の両面から検討すべきである。

まず、プライバシー侵害にあたるかどうかについては、取得型のプライバシー侵害に関する裁判例、ことに不特定多数を対象に網羅的に情報を取得するケースについて争われた、警察の車両ナンバープレート読み取りシステム「N システム」に関する裁判例（東京地判平成 13 年 2 月 6 日）[25]が参考になる。判決は、プライバシー侵害 に関する適法性の判断基準として、取得、保有、利用される情報が①個人の思想、信条、品行等に関わるか、などの情報の性質、②目的が正当なものであるか、③方法が正当なものであるか、などを総合して判断すべきとした。この事案については、裁判所は N システムによる権利侵害は認められないと結論づけたが、「仮に、N システムの端末が道路上の至る所に張りめぐらされ、そこから得られる大量の情報が集積、保存されるような事態が生じれば、運転者の行動や私生活の内容を相当程度詳細に推測し得る情報となり（略）目的や方法の如何を一切問わず収集の許される情報とはいえないことも明らかである」などとして、網羅的な情報収集が権利侵害となる場合があることを正面から認めている。

N システム事件で裁判所が使用した基準を本件にあてはめてみれば、以下のようになるであろう。①の情報の性質については、ウェブの閲覧履歴であり、一般に個人の思想、信条、品行等を推知しうるものであるうえ、「いいね！ボタン」の設置基準が定められていないためアダルトサイト閲覧などの履歴も収集されてしまう。②は、広告目的であり、人の生命、身体、財産の保護を目的とする防犯等に比べればその重要性は一段落ちるものである。さらに、③の方法については、前記のとおり、(a)「いいね！ボタン」の設置されたウェブサイトを閲覧しただけで閲覧履歴が収集されることはユーザーにとって不意打ちの恐れがあること、(b)オプトアウトが認められていないこと、などから取得方法の正当性には疑問がある。以上の点から、FB による情報収集がプライバシー侵害にあたると判断される可能性は、N システム事件が警察による情報収集であるという点を考慮してもなお、十分にあるというべきである。

次に、個人情報保護法違反の可能性については以下のとおりである。本件についての見方として、理論的には（ア）FB を個人情報の取得の主体とし、ボタン設置サイトを FB か

---

[24] 前掲注 19。

[25] 東京地判平成 13 年 2 月 6 日、判例時報 1748 号 144 頁。本件の評釈として、小林直樹「N システムと自己情報コントロール権」法律時報 78 巻 8 号（2001 年）80 頁。

ら取得の委託を受けたものとする見方と、（イ）ボタン設置サイトが一旦、個人情報を取得し、後に FB にその情報を提供した、とみる見方があり得るが、まず、（ア）について考えたい。

（ア）のケースでは「個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない」と定める第 17 条第 1 項に抵触する可能性が考えられる。

第 17 条第 1 項は、OECD8 原則の一つ、「適法かつ適正な手段」による収集でなければならないという「収集制限の原則」と同趣旨で、例えば本人に対して個人情報を収集しているという事実を偽って取得する場合などが想定されるとされる [26]。

「いいね！ボタン」はその形状や名称から、あたかも、閲覧者がクリックした場合にのみ何らかの動きが起きると想像させるが、実際にはクリックの有無にかかわりなく、閲覧した瞬間に FB のサーバーにブラウザがアクセスし、閲覧者が FB 会員の場合は結果として個人情報が取得される形となっている。これが多くの一般人の予想を裏切るものであることは、閲覧者はもとより、ボタンを設置するサイト運営者の多くが、閲覧するだけで情報が送信されると認識していなかったことからも明らかである。2018 年 1 月時点の売上高上位 100 社の調査では、自社のウェブサイトに外部の広告会社やアクセス解析会社の JavaScript を設置して閲覧者のクッキーデータをそれらの会社に送っている場合にプライバシーポリシーにその旨の記載をしている企業であっても、同じ仕組みである「いいね！ボタン」について記載しているケースは見つからなかった。これは「いいね！ボタン」の情報送信機能を把握していなかったことの現れとも考えられる。例えば、ある大手自動車メーカーは読売新聞の取材に対し、「商品の宣伝になると思って設置しただけで、まさか閲覧するだけで情報送信させる仕組みとは思わなかった」と回答している [27]。

個人情報保護委員会は、2018 年 10 月 22 日付で FB に対し「いいね！ボタン」問題を含む 3 件の事案を理由に個人情報保護法に基づく行政指導を行った [28]。これは FB の利用者への説明や同意の取り方が不適切であり、第 17 条第 1 項の適正取得義務に違反する恐れがあると判断したためと推測される。

一方、取得の「入り口」となるボタン設置サイトの運営者に法的責任はないのであろうか。この構図は、スマートフォンでアプリを使用した際、アプリ提供事業者がアプリに組み込んだ広告会社などの情報収集モジュールによって、利用者のデータが広告会社などの第三者に送信されるケースと似ており、この問題について検討した総務省の有識者会議の報告書「スマートフォン・プライバシー・イニシアティブ（SPI）」[29]が参考になる。

報告書では、「情報収集モジュール提供者は、一般に利用者に対する接点を直接持っておらず、利用者側も何の情報収集モジュールが入っているか等の情報を提供されない限り知

---

[26] 園部逸夫・藤原静雄編『個人情報保護法の解説』（ぎょうせい、2018 年）148 頁。
[27] 前掲注 19。
[28] 個人情報保護委員会「個人情報の保護に関する法律に基づく指導について」。
https://www.ppc.go.jp/news/press/2018/20181022/
[29] 総務省「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会・スマートフォンを経由した利用者情報の取扱いに関する WG 最終取りまとめ・スマートフォンプライバシー　イニシアティブ」（2012 年 8 月）。
http://www.soumu.go.jp/main_content/000171225.pdf

り得ず、情報収集モジュール提供者のウェブページを参照する等の措置もできない。また、情報収集事業者や広告配信事業者等による情報収集モジュールの配布を通じた情報取得については、情報収集モジュールをアプリケーション提供者へ配布しこれをアプリケーション提供者がアプリケーションに組み込むことによって可能となるが、情報収集モジュールの中には、アプリケーション提供者により一部変更されて組み込まれているものもあり、変更内容についてアプリケーション提供者でないと正確に分からない場合もあると指摘される。このため、詳細は情報収集モジュール提供者が掲載するプライバシーポリシー等を通知又は公表し説明する必要があるものの、アプリケーション提供者のプライバシーポリシーにおいて情報収集モジュール別に最低限必要な情報を利用者に通知又は公表するなど、アプリケーション提供者と情報収集モジュール提供者の間の役割分担により透明性を高めることが現実的かつ必要ではないかとの指摘がある」[30]と書かれている。

さらに、「アプリケーション提供者が本人に対して適切な説明をしていないことを知りつつまたはそのことを知るべくして必要な対策を講じることなく、情報収集モジュールを配布し、結果として、本人の認識なくアプリケーションから情報を取得することは、第 17 条の違反となる可能性があると指摘される」[31]とも記載している。

この検討結果におけるアプリ提供者を「いいね！ボタン」設置サイトに、情報モジュール提供者を FB に、それぞれ当てはめた場合、利用者へのわかりやすい通知なしに「いいね！ボタン」を設置することは、FB のみならず、「いいね！ボタン」の設置サイトの事業者も個人情報保護法第 17 条違反に該当する可能性があることが示唆される。

個人情報保護委員会は、「いいね！ボタン」問題を受け、委員会ホームページ上で注意喚起 を掲載[32]し、ボタン設置のサイト運営者に対し、①閲覧するだけで利用者のブラウザ等の情報が送信されてしまうこと、②送信先事業者の保有情報によっては個人情報にあたる可能性があること、などを理解するよう求め、それでも設置する場合にはプライバシーポリシーに分かりやすく記載するよう注意喚起したが、これは前述の SPI の見解と同趣旨のものと思われる。

しかし、FB が情報取得の主体であり、ボタン設置サイト運営者は FB から情報取得を委託された者である、とみる考え方は、利用者の立場に立つと分かりにくいという問題がある。利用者が能動的にアクセスしているのは、あくまでボタン設置サイトであり、ブラウザが裏で FB のサーバーにもアクセスしていることに気づくのは難しい。利用者にすれば、実質的には、ボタン設置サイト運営者にブラウザ情報を取得され、ボタン設置サイトから第三者である FB に提供されたと考える方が自然であるとの見方もある。したがって、このような見方を取れば前述（イ）の理解に立つことになるが、この場合の法的問題については６．において後述する。

４．３．DMP 事業者によるデータ提供

前述の通り、DMP と呼ばれるプラットフォームのうち、パブリック DMP を提供する事

---

[30] 前掲注 29　49 頁。
[31] 前掲注 29　50 頁脚注 17。
[32] 個人情報保護委員会「SNS の「ボタン」等の設置に係る留意事項」。
https://www.ppc.go.jp/news/careful_information/sns_button/

業者は、様々な事業者から集めたクッキーや広告 ID、または DMP 事業者が振った ID に紐付くユーザーデータを集め、統合、分析し、さらには外部に提供している。そのデータ量は膨大で、国内のパブリック DMP 最大手「インティメート・マージャー」の場合、4.7 億ブラウザの情報を保有するとうたっている[33]。こうして集められたデータは、性別、年齢、職業、家族構成、居住地区、趣味など多岐にわたって分類され、例えば趣味も、単に「スポーツ」だけでなく、ゴルフ、登山など詳細なセグメントに区分され、同社の場合、5,000 を超えるセグメントで区分している[34]

これらのデータは、クッキーなどの識別子に紐付いた情報であり、それ自体は個人情報ではない。しかしながら、顧客情報を保有する事業者に提供され、顧客情報と突合させれば個人情報に変わりうるものであることは、これまで述べてきた通りである。そして実際に、「顧客情報の拡張」をうたい文句として、顧客情報を保有するユーザー企業への営業を展開している DMP 事業者もいる。

例えば、DMP 事業者トレジャーデータは同社のウェブサイト上で、データ活用のための同社のツールを導入した国内大手の飲料メーカー、キリンの事例として、キリンの担当者へのインタビュー形式で以下のような紹介をしている[35]。

「そこで今年から導入したのが、トレジャーデータが提供するデータマーケティング基盤『TREASURE CDP』だ。TREASURE CDP は、オウンドメディアのアクセスログ、広告配信ログ、CRM のコミュニケーションログなど企業が保有する顧客データだけでなく、セカンドパーティ・サードパーティの DMP が提供するオーディエンスデータを収集・統合管理してデジタルマーケティングのパーソナライズを可能にする。外部データを自社の顧客データと統合することで、顧客の姿をより鮮明にしようと考えたのだ」「他のデータとのマッチングがしやすくなることで、顧客のことをどんどん深堀して理解できるようになります」

同サイトでは、大手化粧品会社、資生堂の事例も以下のように紹介している[36]。

「顧客が「ワタシプラス」[37]に履歴を残したとしても、その足跡は実際のユーザー行動のうちごく僅かなものだということ。当然のことながら、顧客は総合美容情報サイトや競合他社のサイトも利用するものだ。つまり、「モーメント」は「ワタシプラス」の外側にも存在する。この「ワタシプラス」の外側のモーメントを、パブリック DMP のデータや、

---

33 株式会社インティメート・マージャー「ニュース」（2018 年 1 月 25 日）。
https://corp.intimatemerger.com/archives/2041/
34 株式会社インティメート・マージャー「ニュース」（2016 年 4 月 14 日）。
https://corp.intimatemerger.com/archives/1855/
35 トレジャーデータ株式会社「事例・顧客　キリン株式会社様」（最終アクセス日 2019 年 1 月 6 日）。
https://www.treasuredata.co.jp/customers/kirin/
36 トレジャーデータ株式会社「事例・顧客　株式会社資生堂様」（最終アクセス日 2019 年 1 月 6 日）。
https://www.treasuredata.co.jp/customers/shiseido/
37 ワタシプラスとはオンラインショップなどの機能をもつ資生堂のウェブサービスで、氏名や年齢、住所などの個人情報を登録して利用する。
株式会社資生堂「ワタシプラストップ」（最終アクセス日 2019 年 1 月 6 日）。
https://www.shiseido.co.jp/wp/index.html

提携サイトのデータ、リアルでの行動データなどを使って捉えたいと考えたのだ。この課題を解決するために、資生堂が導入したのがカスタマー・データ・プラットフォーム「TREASURE CDP」だ。同社が「TREASURE CDP」を 導入した理由は大きく 3 つ。どのような形のデータでも大量に保存ができること。ログデータの収集が容易に行えること。外部サービスとの連携が容易に実現できること。」

このように、クッキーなどの識別子に紐付く個人に関する情報を、個人情報を保有する企業に対し、個人情報の拡張を予想しつつ、あるいは、それを営業のセールスポイントとして提供するプラットフォーム事業を展開しているのである。

なお、トレジャーデータ、キリン、資生堂のそれぞれのプライバシーポリシーには、トレジャーデータが提供するプラットフォームによってキリンおよび資生堂が個人情報を拡張している旨の記載は見当たらなかった [38]。

４．４．DMP 事業者のデータ提供の法的評価

FB の事例では取得型のプライバシー侵害について検討したが、ここでは、提供型のプライバシー侵害について考える。提供型について裁判例の多くは、①一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められる事柄を提供・公開される場合にプライバシー侵害を認めている。ただし、②その情報が誰の情報か分からない匿名情報である場合にはプライバシー侵害にはあたらないとする事例が散見される [39]。

---

[38] トレジャーデータ株式会社「個人情報保護指針」（2017 年 8 月 1 日制定）。
https://www.treasuredata.co.jp/privacy/policy/
トレジャーデータ株式会社「個人情報に関する公表文」（最終アクセス日 2018 年 1 月 6 日）。
https://www.treasuredata.co.jp/privacy/policy-2/
キリン株式会社「個人情報の保護」（制定日 2015 年 10 月 1 日）。
https://www.kirin.co.jp/privacypolicy/index.html?_ga=2.241875015.495549814.1541341639-1738990029.1531286439
株式会社資生堂「個人情報について」（最終更新日 2018 年 10 月 3 日）。
https://www.shiseidogroup.jp/privacy-policy/

[39] 例えば、複数の記事に関する、名誉毀損・プライバシー侵害が争われた事案において、一部の記事について、「匿名性が認められる以上、名誉毀損のみならず、プライバシーの侵害についても、成立する余地がない」と判示したものがある（東京地判平成 6 年 4 月 12 日　判例集未登載）。また、川崎市が市職員に対し政党機関誌の購読調査を行ったことに対し、当時の市職員らがプライバシー侵害などを理由に提訴した損害賠償請求事件では、横浜地裁川崎支部は回答が匿名だったことを理由にプライバシー侵害を否定し、控訴審も原審の判断を支持している（横浜地裁川崎支部判決平成 21 年 1 月 27 日、東京高判平成 23 年 9 月 29 日　いずれも判例集未登載）。さらに、防衛庁の職員が防衛庁に対する行政文書開示請求者のリストを作成し庁内に配布したことが、リスト記載者のプライバシーの侵害にあたるかが争われた事案において、リストの作成により原告のプライバシーが侵害されたというためには、「そのリストに記載された原告に関する個人情報が個人識別性を有することが必要である。そして、当該個人情報の開示によりプライバシーが侵害されたか否かが問題となる場面における個人識別性については、当該情報のみで識別でき

DMP 事業者のケースでは、提供される属性データは、詳細なウェブの閲覧履歴に基づくもので、本人の趣味・嗜好、生活様式に加えて思想・信条にかかわるものまで含みうるものであるため、①のケースに該当する事柄であるといえよう。さらに、②について検討すると、提供先の企業においては、提供された情報がどの会員のものか特定できてしまう性質のものであるため匿名情報ではない。従って、DMP 事業者による属性データの提供は、それが提供先で個人情報となる場合、プライバシー侵害と評価される可能性がある。

サードパーティクッキーを利用した情報収集には、かねてプライバシーの問題があるとされながらも、それが匿名状態での収集であることから、個人情報保護法に抵触せずプライバシー侵害にも当たらないとして許容されてきた面がある。しかし、収集された情報を意図的に個人情報と結合・突合するならば、その行為は、許容されてきた一線を越えるものであるように思われる。個人情報保護法上の評価については、６．において後述する。

５．海外の規制

欧州連合（EU）では 2018 年 5 月 25 日、GDPR（General Data Protection Rules・一般データ保護規則）の適用が開始された。EU ではこれまで、1995 年に制定されたデータ保護指令の下で各国が国内法を制定してきたが、GDPR は EU 単一のルールとして加盟国に直接に適用される。

GDPR ではこれまでより事業者に対する制裁が強化され、データポータビリティの権利や忘れられる権利なども新たに盛り込まれたが、保護すべきデータの定義は従前通りである。個人データは「識別された、または識別され得る自然人（「データ主体」）に関するすべての情報」と定義され、例えば、「自然人の氏名」や「識別番号」「所在地データ」などのほか、「メールアドレス」「オンライン識別子(IP アドレス、クッキー識別子)」「身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因」なども含まれる [40]。

個人データの取得や第三者提供などは、個人データを取り扱う行為はすべて「処理」と定義され、処理が適法となる場合は限定列挙されている。データ主体の同意がある場合のほか、「正当な利益」のために処理が必要な場合にも処理が適法となる。「正当な利益」の中には「ダイレクトマーケティングのための処理」も含まれるとされており [41]、広告配信のための収集が適法とされるかどうかは今後の動向に注視する必要がある [42]。

る場合に限らず、一般人が特別な調査を要せずに容易に入手し得る他の情報と照合することにより当該個人を識別できる場合も、これを肯定するのが相当である」として個人識別性の基準を提示したうえで、この基準により個人識別性を認められない原告についてのプライバシー侵害を否定したものがある（新潟地判平成 18 年 5 月 11 日　判例集未登載）。

[40] 森大樹編集代表『日米欧　個人情報保護・データプロテクションの国際実務』（商事法務、2017 年）。

[41] 個人情報保護委員会「一般データ保護規則前文（和訳）」。
（47）「ダイレクトマーケティングのための個人データの取扱いは、正当な利益のために行われるものとみなされうる」。
https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf

[42] 一般データ保護規則第 6 条第 1 項（ｆ）では、適法とされる取り扱いについて「管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要と

GDPR とは別に、現行の「e プライバシー指令」（e Privacy Directive）に代わる「e プライバシー規則」（e Privacy Regulation）が成立間近とされている（2018 年 6 月 28 日現在、欧州議会は承認したものの、EU 理事会の審議がまだ続いている）。通信当事者のデータを保護するために取扱事業者を規制するもので、成立すれば、現行の指令が対象としている通信会社のほか、FB や WhatsApp、Skype など、ネット上のメッセージや音声のサービス提供事業者にも適用されることになる。特にサードパーティクッキー等を使った情報の取得や提供を含めたデータの処理には利用者の事前同意を義務づけてオプトアウトは認めず、違反すれば制裁金が課されることになる見通しである [43]。

一方、ベルギーでは、2015 年 11 月、情報保護当局（the Commission for the protection of privacy (CPP)・現 the Data Protection Authority（DPA））が FB を相手取って起こした訴訟で、FB が「いいね！ボタン」を設置した外部サイトでの閲覧履歴を追跡し、FB 利用者以外のユーザーも含めて閲覧履歴を追跡していたことについて、ベルギーの裁判所は同国の情報保護法に違反しているとの判断を示した [44]。FB が登録情報を持たない FB 利用者以外の閲覧履歴は、日本の個人情報保護法では個人情報には該当しないが、ベルギーの裁判所はクッキーなどのオンライン識別子も保護すべきであるとして、このような判断を示したと考えられる。

米国では米国連邦取引委員会（FTC）が 2010 年、ウェブ上のトラッキングを拒否する「Do Not Track」の仕組みをブラウザの機能の一部として追加するよう勧告している。既にこの機能がデフォルトでオンになっているブラウザもあるものの、対応しないことをプライバシーポリシー等で宣言する運用も許容されている。また、2015 年 2 月に提案された「消費者プライバシー権利章典法案」では、個人データの定義を「その事業者によって特定の個人に連結若しくは実際に連結可能な、又は日常的に利用されている機器に連結された全てのデータ」[45]で、具体例として端末 ID も列挙されたが、法制化の目途は立っていない。

６．提供先で個人識別性を獲得する提供行為の評価

これまで述べてきたように、インターネット広告の世界では、収集の「入り口」においては非個人情報でも、第三者に提供された結果、提供先の事業者が保有する情報によっては、個人を特定する情報に変わりうる。DMP 事業者が端末やブラウザに紐付けられた情

なる場合」としながらも、「ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く。」と続けており、ダイレクトマーケティングの正当性が認められるかどうかは必ずしも確定的ではないとの見方がある。
個人情報保護委員会「一般データ保護規則条文（和訳）」。
https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

[43] European Commission 「Proposal for an ePrivacy Regulation」
https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[44] Data Protection Authority 「The judgment in the Facebook case」
https://www.dataprotectionauthority.be/news/judgment-facebook-case

[45] 瓜生和久編著『一問一答平成 27 年改正個人情報保護法』（商事法務、2015 年）16 頁。

報を、顧客情報を保有する企業に提供するケースが典型的である。また、FB の「いいね！ボタン」のケースも、FB が個人情報取得の主体で、ボタン設置サイト運営事業者が取得の委託を受けているとの見方がある一方で、ボタン設置サイト運営事業者が取得した非個人情報を第三者である FB に提供した結果、FB において個人情報に変わったと見ることもできる。

そこで、こうした状況に対する、個人情報保護法第 23 条の第三者提供に関する規制の適用可能性について考えたい。

個人にかかわる情報が同法で保護対象としている個人情報に該当するかどうかは、原則として事業者ごとに相対的に判断されるものである[46]。例えば、前述したように、いろは商事の「社員番号 12345」という情報は、社員名簿を保有するいろは商事にとっては、特定の個人を識別する情報であるが、これが別の会社に提供されたとしても、個人識別性はないといったことが想定される。

第三者提供の場面において、容易照合性の判断基準を提供元に置くか、提供先に置くかについては、2013 年に JR 東日本による Suica 乗車履歴データの第三者提供が問題となった事案などを機に議論が起きている。岡村久道らは提供先において特定の個人が識別できる場合に限り適用されるべきであるとする「提供先基準説」[47]を唱え、これに対し、高木浩光らは提供元において特定の個人が識別される場合には同規制が適用されるという「提供元基準説」[48]を主張したが、現在は提供元基準説が通説[49]となっており、政府の国会答弁[50]もこの立場を支持している。ただ、この時の議論は、提供元において個人識別性を有するケースを前提として行われたものである。岡村らの主張の趣旨は、提供元では個人識別性のある情報でも、提供先においては個人識別性がない状態（以下、この場合を「提供元〇提供先×」とする。）であれば第三者提供の規制対象としなくてもよい、というものであった。これに対し、高木らが主張し、通説となった提供元基準説は「提供元〇提供先×」のケースについても規制対象とするというものであった。しかしながら、インターネット

---

46 例外として個人識別符号、顔画像、氏名等は、すべての事業者との関係で個人情報である絶対的個人情報である。

47 岡村久道「パーソナルデータの利活用に関する制度見直しと検討課題（中）」NBL 1020 号（2014 年）73 頁。

48 高木浩光「高木浩光@自宅の日記」（現行法の理解・2014 年 4 月 23 日）。
http://takagi-hiromitsu.jp/diary/20140423.html

49「個人情報の保護に関する法律についてのガイドライン（通則編）（案）」に関する意見募集結果「ある情報を第三者に提供する場合、当該情報が「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる」かどうかは、当該情報の提供元である事業者において「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる」かどうかで判断します。」。

50 2015 年 5 月 28 日参議院内閣委員会（政府参考人向井治紀）「日本の個人情報の定義は、容易に照合できる、他のデータと合わせて個人が識別できるものというふうになっているところでございます。その際に、情報を移転する際に、容易に照合するのは情報の移転元か移転先かという議論がございます。日本の場合、これは情報の移転元で容易照合性があるということで解釈が統一されておりまして、そういたしますと一旦個人情報となりますと、その情報の一部を提供する場合でもこれは大抵の場合、提供元において容易照合性はありますので、個人情報になってしまうという、そういうことはございます」。

広告の世界でしばしば生じている、「提供元において個人識別性がないが、提供先において個人識別性がある」（以下、この場合を「提供元×提供先○」とする。）というケースについては、これまで十分な検討がなされてこなかったのである。

そこで本稿では、「提供元×提供先○」のケースについても、第三者提供に関する個人情報保護法第23条の規制が適用すべきかどうか、正面から検討することとする。さらには、「提供元○提供先×」という従来の議論の対象となったケースについても、通説である提供元基準説に再考の余地がないか検討することとする。

まず、「提供元×提供先○」のケースについて、第23条を適用すべきかどうか。これについては、本稿の3人の共同執筆者の間で意見が分かれた。

執筆者のうち1名は、「提供元×提供先○」のケースにおいては提供元基準を維持し、第23条を適用すべきでないとの意見であった。これは、①提供元基準を一貫させる方が法的安定性に資すること、②提供先で個人識別性を有する情報となって個人情報に該当するようになることについては、取得の規制（第17条の適正な取得、第18条の取得に際しての利用目的の通知等）により対処すれば足りること、③提供元では、提供先で「個人情報」に該当するか否かが必ずしも判断できないこと、および④第23条第1項の文言は、「個人情報取扱事業者は（中略）個人データを第三者に提供してはならない」であるところ、事業者にとって個人データでないものを提供する行為は本稿の解釈を超えるとの主張であった。

これに対して、執筆者のうち2名が主張した「提供元×提供先○」のケースにも第23条を適用すべきとする理由は、以下のとおりである。そもそも提供元が提供行為を行わなければ、提供先の権利侵害の恐れは発生しないのであるから、提供元の提供行為こそが権利侵害の原因である[51]。したがって権利侵害の原因となる提供元の行為に対する規制を行わずに、提供先に対する取得規制のみの問題とすることは適当ではない。提供先において個人識別性がある場合に権利利益の侵害のおそれがあることを考えれば、「提供元×提供先○」のケースにおいても、第23条の規制を適用すべきである。

ただ、通常は提供元からみて提供先における個人識別性があるか否かが明確でないということは、第23条の適用に際して障害となりうる。しかし、提供元において、提供する情報が、提供先で個人識別性を獲得する蓋然性が高いことを認識しているのであれば、当該提供行為は、実質的に個人識別性のある情報の提供行為と同様であると評価することが可能である。従って、提供元があらかじめ、その情報が提供先で個人識別性を獲得することを知っている場合、または容易に知りうる場合には、個人識別性のある情報の提供と同様であると評価して、第23条を適用すべきである[52]。なお、第23条第1項の「個人データを第三者に提供してはならない」との文言との関係では、提供元において個人データでない情報を、提供先において個人データになることの認識と共に提供先に提供する行為は、

[51] たとえば、3．2．で紹介したピギーバックのケースのように、一つのウェブサイトを閲覧したことにより、大量のサードパーティに閲覧履歴の提供がなされるような場合には、この問題は顕著である。

[52] 「いいね！」ボタン設置者による提供行為が認められるかについては、議論がありうるが、本人による追跡可能性を考えれば、提供行為を認めたうえで第23条を適用することが適切であるとの立場もありうる。

「個人データを提供」することにあたると解することは十分に可能というべきある。メールアドレスや広告 ID といった共用性のある識別子と共に個人に関する情報が流通するようになった今日においては、提供元で個人情報でないものが提供先で個人情報となることは、しばしば起こりうることであり、これを第 23 条第 1 項の「提供」から除外する解釈は、かえって本稿の趣旨を損なうこととなるであろう[53]。

第 23 条との関係で提供先における権利利益の侵害のおそれを重視し、「提供元×提供先○」のケースにおいて提供元基準を否定する考え方を採る場合、従来は「提供元○提供先×」においても提供元基準説に基づくべきとされていたことについて見直すべきかどうかも、検証を試みる必要があるだろう。より具体的には、提供先では個人識別性がないことが明白な場合等については、第 23 条の適用除外とすべきか、という点が問題となる。

ここにおいても、通常、提供元からみて提供先における個人識別性があるか否かを知っているか、または容易に知りうるかという点が重要になるだろう。なぜなら、仮に提供元が、「提供先において、個人が識別される可能性は全くない」と合理的に判断できるのであれば、そのような提供は、実質的には権利利益の侵害の恐れを伴うものではないからだ。

しかしながら、この「提供先において個人識別性を獲得するか否か」という問題は、実のところ、匿名加工情報の制度導入にあたって議論されてきた問題でもある。匿名加工の中心的課題は、いかにして提供先において個人識別性を持たないような情報に加工するか、というものであったが、個人情報保護法改正の前に匿名化の加工技術について検討した技術ワーキンググループは、報告書[54]で「情報の利活用における有用性を全く失うことなく、いかなる個人情報をも対象にした汎用的な匿名化手法はない」と結論づけたのである。改正法が第 38 条で匿名加工情報取扱事業者に対し、本人を識別するための照合を禁じているのも、完全な匿名化の技術は存在しないからであるともいえる。つまり、個人情報にどれほど加工をほどこしたとしても、一意な部分が残る限り、提供先で個人識別性を有する情報になる可能性は消えないということである。この認識の下で、第 23 条の同意を不要として第三者に提供する場合は、匿名加工情報の制度によるべきであるというのが、現行法の考え方である。従って、それ以外の方法で匿名化した個人情報（一意の部分が残る場合）の第三者提供を第 23 条第 1 項の対象外とすることは適当ではない[55]。したがって、「提供元○提供先×」の場面においては、提供元基準説を修正する必要はないと考える。

以上をまとめると、「提供元×提供先○」のケースにおいては共同執筆者間で見解が分かれ、提供元基準を一貫し第 23 条を適用すべきでないとする意見と、情報が提供先で個人識別性を獲得することを、提供元が知り、また容易に知りうる場合には、第 23 条を適用すべきであるとする意見があった一方、「提供元○提供先×」のケースにおいては、共同執筆

---

[53] たとえて言えば、「まずい食べ物を人にあげてはいけない」という禁止について考える場合、提供元が個人的に嫌いなものを提供してはいけないという解釈も可能であるが、他方で、一般には「まずい食べ物」とされていないものであっても提供先が好まないことを知っている場合には、この禁止が及ぶと解することは十分に可能である。

[54] 技術検討ワーキンググループ「報告書」（2013 年 12 月）27 頁。
「https://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf

[55] もっとも、全データで K＝２以上の匿名化をする場合には、物理的に再識別の可能性がなくなるため、この限りではない。

者全員が従前どおりの提供元基準説を維持し、常に第 23 条を適用すべきであるとの結論となった。

7．おわりに

インターネット広告により、広告の効果や利便性は増しているが、一方で、広告事業者が扱う個人に関する情報は膨大になり、本人が関与することができない状態のまま多数の事業者間を流通している状態である。これらの情報は、取得の「入り口」において、ブラウザや端末の識別子に紐付いた情報として取得されるため、個人情報保護法の規制を受けず、それゆえに本人が気付きにくく関与しにくいという問題がある。本稿ではさらに、そのうちの一部は、保有する組織によって個人情報に変わり、本人が自己の個人情報が収集・保有されていると気付くことが難しいという問題があると考え、これに対して、個人情報保護法を中心とした現行法で対応する場合のアプローチについて検討してきた。

FB のようなケースについては、本人にわかりやすい説明や同意をとらなければ個人情報保護法第 17 条の適正取得義務違反に問うというアプローチがあり得る。また、DMP 事業者が提供先で個人情報になることが予想される相手に提供するような事例に対しては、「提供元×提供先○」のケースにおいても第 23 条を適用することで規制する可能性を検討した。

本稿の中心的テーマは現行法の下でのアプローチであったが、将来的には、端末やブラウザの識別子について法的扱いを見直すべきではないかと考える。

「特定の個人を識別する」という個人情報の定義中の「特定」は、かつては氏名到達性を重視して論じられる傾向にあったが、技術の進展により、その意味するところは変わりつつあると言っていいだろう。サイバー空間での個人の行動が重みを増す中、実社会ではどこの誰か分からなくても、サイバー空間で本人に到達でき、一意性を有するなどの性質をもつ情報であれば、特定性を認めるというのが自然な考え方である。氏名等と結びつくことで、それが実社会におけるある人を指し示す場合のみを個人情報とし、それ以外は対象から外すという整理には限界が来ているのである [56]。平成 27 年改正法で新たに個人情報の概念として加えられた個人識別符号は、氏名等に結びつくかとは無関係に、一意性を有するか、簡単に変更することができないか、本人に連絡できるか等の要素を基準に一定の符号が個人情報でありうることを確認したものである。端末識別子も、これに加える方向で見直しをするべきであると考える [57] 。さらには、「それが誰か一人の情報であること

[56] その典型は、メールアドレスについて「ユーザー名及びドメイン名から特定の個人を識別できる場合」のみ単体で個人情報にあたるとする従来の考え方である（個人情報保護委員会 Q&A1-4）。

[57] 言うまでもなく、このような規制強化は、国内市場で活動する外国事業者に対して第 75 条の域外適用規定等を用いた法執行が実効的に行われることを前提とする。端末等の識別子に紐付く国民の個人情報は、外国事業者によっても大量に取り扱われており、内外事業者間の公正競争の問題を別にしても、これらの外国事業者に対する法執行がなされなければ国民の権利利益の保護の実を上げることにはつながらないのである。このような内外事業者へのイコールフッティングの必要性を指摘するものとして、森亮二「データ活用ビジネスとプライバシー問題」ビジネスロージャーナル 2013 年 1 号（2013 年）27 頁。

がわかるが、その一人が誰であるかまではわからない情報」（識別非特定情報[58]）についても保護対象とするかどうかの検討が急がれるだろう。いったんは識別非特定情報と判断されたとしても、同じ識別子で蓄積される期間や特徴的な属性の有無や量、刻々と向上しているプロファイリング精度等に応じて照合精度が高くなり続けることを考慮すべきだ。

なお、現在インターネット広告については、業界別の様々な業法における規制が存在している。具体的には医薬品医療機器法、健康増進法、金融商品取引法などである。業種横断の一般的な広告規制としては、景品表示法や特定商取引法によるものが挙げられる。しかし、これらはすべて表示内容の適正さに関する規制であり、プライバシーの観点から広告を規制するものではない。インターネット広告事業者などで作る一般社団法人「日本インタラクティブ広告協会（JIAA）」は「行動ターゲティング広告ガイドライン」や「プライバシーポリシー作成のためのガイドライン」[59]を作成しているが、あくまでガイドラインであって強制力があるものではなく、もとより、海外企業や非加盟社などが従わないことは当然予想されるところである。

こうした現状に鑑み、端末識別情報等の流通に対して、利用者本人が関与できる仕組みを作る必要がある[60]。そのために、法改正も視野に入れながら、本稿で論じてきたような個人情報保護法における個人情報の定義や第三者提供の範囲の解釈の見直しにより端末識別情報の提供を規制することを検討する必要があると思われる。

主要参考文献

・一般社団法人日本インタラクティブ広告協会（JIAA）「インターネット広告の基本実務 2016 年度版」（JIAA、2016 年）
・曽我部真裕・林秀弥・栗田昌裕『情報法概説』（弘文堂、2016 年）
・園部逸夫・藤原静雄編集『個人情報保護法の解説』（ぎょうせい、2018 年）
・森亮二「インターネット広告に関する最近の法律問題」国民生活研究第 56 巻第 2 号（2016 年 12 月）47~62 頁

（掲載決定日：平成 31 年 1 月 15 日／オンライン掲載日：平成 31 年 2 月 15 日）

---

58 パーソナルデータに関する検討会・技術検討ワーキンググループ報告書（2013 年 12 月 10 日）
http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf

59 日本インタラクティブ広告協会　ガイドライン。
http://www.jiaa.org/release/release_guide_140324.html

60 法規制の動きとして、カリフォルニア州では 2018 年に消費者プライバシー法案が成立した。同法では、端末識別情報等に消費者が関与できることを規定しており、「実名、別名、郵便アドレス、固有の個人識別子、オンライン識別子、インターネットプロトコルアドレス、電子メールアドレス、アカウント名、社会保障番号、運転免許証番号、パスポート番号または他の類似の識別子などの識別子」を個人情報に含むとしている。